Quantum Kolmogorov Complexity and Bounded Quantum Memory

Takayuki Miyadera
Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST).
Daibiru building 1003, Sotokanda,
Chiyoda-ku, Tokyo, 101-0021, Japan.
(E-mail: miyadera-takayuki@aist.go.jp)
(Dated: February 9, 2011)

In this study, the effect of bounded quantum memory in a primitive information protocol has been examined using the quantum Kolmogorov complexity as a measure of information. We employed a toy two-party protocol in which Bob by using a bounded quantum memory and an unbounded classical memory estimates a message that was encoded in qubits by Alice in one of the bases X or Z. Our theorem gave a nontrivial effect of the memory boundedness. In addition, a generalization of the uncertainty principle in the presence of quantum memory has been obtained.

PACS numbers: 03.67.Lx, 03.65.Ta, 03.67.Dd

I. INTRODUCTION

Various ideas have been put forth and experiments have been conducted to construct a large and stable quantum memory. This is definitely the most important factor for achieving quantum information processing devices. However, despite the efforts expended thus far, it is difficult to imagine that any ultimate method will be proposed that enables the construction of an arbitrarily large quantum memory.

This pessimistic view is not as disappointing as it may seem. Let us consider a two-party cryptographic protocol called oblivious transfer [1], in which Alice sends a bit to Bob by executing a protocol in such a manner that Bob receives it correctly with probability 1/2 and nothing otherwise, but Alice cannot learn whether her bit was received. While the oblivious transfer could be a strong cryptographic primitive when realized, its secure realization without considering any assumptions is impossible even if one uses quantum communication [2, 3]. Several studies have been conducted to investigate physical assumptions yielding the secure implementation of this protocol using classical communication. The first assumption is the boundedness of computation power, which is the most traditional approach based on a mathematically unproven computational complexity problem [1]. This approach implicitly contains a physical assumption: it assumes the processing speed of existing computers. The second assumption involves the imperfection of a communication channel. It has been demonstrated in various noise models that secure oblivious transfer is achievable [4, 5]. The third assumption, which is related to the present study, is the boundedness of memory size. It has been shown that the protocol may be securely implemented if the size of an adversary's (classical) memory is restricted [6]. Although this result is interesting in theory, the assumption is not entirely valid because it is not too difficult to construct large classical memories with current technology. Recently, important work based on bounded quantum memory has been completed. In [7], Damgaard et al. have shown that the oblivious transfer becomes information-theoretically secure under the assumption that the size of the adversary's quantum memory is bounded. As mentioned earlier, the assumption of bounded quantum memory is more reasonable than that of bounded classical memory. In fact, the latest technology enables the stability of only a few qubits of memory.

The protocol runs as follows. Alice encodes a random N bit sequence to a quantum state of N qubits in X or Z basis. She sends the qubits to Bob. Bob selects X or Z and measures the qubits with respect to the selected basis. After Alice announces the basis used for encoding, Bob knows whether his selection of the basis is correct. The privacy amplification phase causes the players to agree on a bit in the case that the basis is correct, otherwise the protocol makes Bob completely ignorant of the bit obtained by Alice. Alice can send Bob an arbitrary bit by XORing with her obtained bit. As intended, this method works as an oblivious channel. To demonstrate the security, assume that one of the players, Bob, is dishonest. If Bob has a quantum memory of size larger than N, he may not follow the protocol but may keep the quantum state and measure it with respect to the disclosed basis. This procedure provides the full information of an encoded sequence to Bob; thus the protocol fails. Further, imagine a case in which dishonest Bob's quantum memory is bounded. Since he cannot keep the entire quantum state, he has to irreversibly convert a part of the quantum state to the classical state by measuring a part of qubits. This operation destroys the quantum state and the information encoded in it. It is essential that he is unaware of the basis used for encoding when the qubits are passed to him. In view of the fact that the noncommutativity of X and Z prohibits their joint measurement, any measurement inevitably induces loss of information. For instance, suppose that Bob with $M(< N)$ qubits memory employs the following simple strategy. When the qubits are sent, Bob keeps the first M qubits as they are and measures the remaining $N - M$ qubits in the Z basis. This strategy allows Bob to obtain full information if

the basis used by Alice for encoding was Z. Conversely, it does not provide full information to Bob if the basis used by Alice was X, because he loses the information that was encoded in the first M qubits. Damgaard et al. [7] has shown that dishonest Bob must have at least $N/2$ qubits quantum memory to benefit in this protocol. That is, the protocol works under the assumption of bounded quantum memory of size smaller than $N/2$.

In this study, we inspect a toy two-party protocol that corresponds to the oblivious transfer protocol with dishonest Bob, but is not followed by privacy amplification. Consider the following problem. Assume that Alice encodes a random N bit sequence to a quantum state in the X or Z basis. How much information can Bob, who has a bounded quantum memory and an unbounded classical memory, retrieve after the basis is announced? By extracting part of a protocol in this manner, it is hoped that the understanding of the power of bounded quantum memory can be deepened. In addition, it may help improve the existing result, as was the case for the quantum key distribution protocol. We study the problem by employing the quantum Kolmogorov complexity as a measure of information, as defined by Vitányi [9]. In contrast to Shannon's theory, which treats only information of probabilistic sources, the Kolmogorov complexity is often called absolute information because it can assign information to individual objects. The key notion is algorithmic randomness. The complexity of an object is defined as the shortest description length in both classical Kolmogorov complexity and quantum Kolmogorov complexity given by Vitányi. While the quantum Kolmogorov complexity is a natural concept for absolute information, it has been used in quantum information theory to develop only a few applications [10, 11] developed in the quantum information theory. One of the purposes of this study is to demonstrate the usefulness of the quantum Kolmogorov complexity for analyzing protocols in this area.

The next section contains a brief review of the quantum Kolmogorov complexity as defined by Vitányi. In section III, we introduce a toy two-party protocol and describe our main result based on it. The conclusion contains a discussion of the results.

II. QUANTUM KOLMOGOROV COMPLEXITY BASED ON CLASSICAL DESCRIPTION

The classical Kolmogorov complexity of a binary sequence is defined by the length of the shortest program, as proposed by Kolmogorov [12] and Chaitin [13] independently, for a one-way Turing machine to output the sequence. For instance, a binary sequence "000...00" has a short description such as "print "0" 10000 times," which therefore has a small Kolmogorov complexity. If a binary sequence has no pattern that yields any compressed description, the best way to describe it is to write it down naively. Such a sequence is called random. That is, a binary sequence is random if and only if its Kolmogorov complexity is as large as its own length. Although a specification of a Turing machine is required to define its value, the Kolmogorov complexity does not depend on the choice of a Turing machine except for a trivial constant. Moreover, the classical Kolmogorov complexity and its conditional version have various rational properties, as do Shannon entropy and conditional entropy. The Kolmogorov complexity plays a central role in field of algorithmic information theory whose applications extend to vast areas such as the foundation of mathematics, computation theory, and physics [14, 15].

While it seems natural to define the corresponding complexity for quantum states, the quantum versions [9, 16–20] of the Kolmogorov complexity were only recently proposed. Among the several versions of the quantum Kolmogorov complexity, we employ the one that was defined by Vitányi [9]. Vitányi's definition based on the classical description length is suitable for quantum information-theoretic problems that normally handle classical inputs and outputs. In order to explain the definition precisely, a description of a one-way quantum Turing machine is needed. A one-way quantum Turing machine consists of four tapes and an internal control. (See [9] for more details.) Each tape is a one-way infinite qubit (quantum bit) chain and has a corresponding head on it. One of the tapes works as the input tape and is read-only from left-to-right. A program is given on this tape as an initial condition. The second tape functions as the work tape. The work tape is initially set to be 0 for all the cells. The head on this tape can read and write a cell, and can move in both directions. The third tape is called an auxiliary tape. One can put an additional input on this tape. The additional input is written to the left-most qubits and can be a quantum state or a classical state. This input is needed when one deals with the conditional Kolmogorov complexity. The fourth tape works as the output tape. It is assumed that after halting the state over this tape will not be changed. The internal control is a quantum system described by a finite dimensional Hilbert space that has two special orthogonal vectors $|q_0\rangle$ (initial state) and $|q_f\rangle$ (halting state). After each step one makes a measurement of a coarse grained observable on the internal control $\{|q_f\rangle\langle q_f|, \mathbf{1} - |q_f\rangle\langle q_f|\}$ to know if the computation halts [21]. A computation halts at time t if and only if the probability to observe q_f at time t is 1, and at any time $t' < t$ the probability to observe q_f is zero (see [22–25] for relevant discussions). By using this one-way quantum Turing machine, Vitányi defined the quantum Kolmogorov complexity as the length of the shortest description of a quantum state. That is, the programs of quantum Turing machine are restricted to classical ones, while the auxiliary inputs can be quantum states. We write $U(p, y) = |x\rangle$ if and only if a quantum Turing machine U with a classical program p and an auxiliary (classical or quantum) input y halts and outputs $|x\rangle$. The following is the precise description of Vitányi's definition.

Definition 1 *[9] The (self-delimiting) quantum Kolmogorov complexity of a pure state $|x\rangle$ with respect to a one-way quantum Turing machine U with y (possibly a quantum state) as conditional input given for free is*

$$K_U(|x\rangle, |\ y) := \min_{p,|z\rangle}\{l(p) + \lceil -\log |\langle z|x\rangle|^2 \rceil : U(p, y) = |z\rangle\},$$

where $l(p)$ is the length of a classical program p, and $\lceil a \rceil$ is the smallest integer larger than a.

The one-wayness of the quantum Turing machine ensures that the halting programs compose a prefix free set. Because of this, the length $l(p)$ is defined consistently. The term $\lceil -\log |\langle z|x\rangle|^2 \rceil$ represents how insufficiently an output $|z\rangle$ approximates the desired output $|x\rangle$. This additional term has a natural interpretation using the Shannon-Fano code. Vitányi has shown the following invariance theorem, which is very important.

Theorem 1 *[9] There is a universal quantum Turing machine U, such that for all machines Q, there is a constant c_Q, such that for all quantum states $|x\rangle$ and all auxiliary inputs y we have:*

$$K_U(|x\rangle|\ y) \leq K_Q(|x\rangle|\ y) + c_Q.$$

Thus the value of quantum Kolmogorov complexity does not depend on the choice of a quantum Turing machine if one neglects the unimportant constant term c_Q. Thanks to this theorem, one often writes K instead of K_U. Moreover, the following theorem is crucial for our discussion.

Theorem 2 *[9] On classical objects (that is, finite binary strings that are all directly computable) the quantum Kolmogorov complexity coincides up to a fixed additional constant with the self-delimiting Kolmogorov complexity. That is, there exists a constant c such that for any classical binary sequence $|x\rangle$,*

$$\min_q\{l(q) : U(q, y) = |x\rangle\} \geq K(|x\rangle|\ y) \geq \min_q\{l(q) : U(q, y) = |x\rangle\} - c$$

holds.

According to this theorem, for classical objects it essentially suffices to treat only programs that exactly output the object.

III. FORMULATION AND RESULTS

In order to discuss the power of the bounded quantum memory, we use a toy two-party protocol. Suppose that there exist two players Alice and Bob. Alice encodes a message in qubits with one of the bases X or Z, and sends them to Bob. The precise formulation is as follows. Alice chooses probabilistically [26] an N-bit message $x \in \{0,1\}^N$. She also chooses a basis X or Z for its encoding. We write the standard basis of a qubit as $\{|0\rangle, |1\rangle\}$, which are eigenstates of Z. Its conjugate basis is written as $\{|\overline{0}\rangle, |\overline{1}\rangle\}$, which are eigenstates of X and are defined as $|\overline{0}\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\overline{1}\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. She prepares a quantum state of N qubits described by a Hilbert space $\mathcal{H}_A$ as follows. If her choice of basis is X, she encodes her message $x = x_1 x_2 \cdots x_N \in \{0,1\}^N$ as $|\overline{x}\rangle := |\overline{x_1}\rangle \otimes |\overline{x_2}\rangle \otimes \cdots \otimes |\overline{x_N}\rangle \in \mathcal{H}_A$. Conversely, if her choice of basis is Z, she prepares $|x\rangle := |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_N\rangle \in \mathcal{H}_A$. We define $X_x := |\overline{x}\rangle\langle\overline{x}|$ for each $x \in \{0,1\}^N$ and $Z_z := |z\rangle\langle z|$ for each $z \in \{0,1\}^N$. Bob, who has a bounded quantum memory and an unbounded classical memory, tries estimating the message after the basis is disclosed by Alice. There may exist some different formulations of the quantum bounded memory. For instance, one of the possible definitions would be such that Bob has many qubits that decohere in an uncontrollable way except for some M qubits. On the other hand, the following definition employed in this paper gives Bob the ability to control the system. Bob has an arbitrarily large system and he makes it interact with the qubits sent from Alice. The whole system that Bob possesses after the interaction is divided into two parts as $\mathcal{H}_m \otimes \mathcal{K}$. The first part is the quantum memory that consists of M qubits. The second part is called an auxiliary part whose size can be arbitrarily large. Because Bob cannot keep the quantum coherence of the auxiliary part, he makes a measurement of an observable on it before the basis is announced by Alice. Let us denote the observable by $C = \{C_\xi\}$, which forms a positive-operator-valued measure (POVM) on $\mathcal{K}$. The measurement result is stored in a classical memory whose size can be arbitrarily large. For as long as he needs, Bob can keep the quantum state on the quantum memory. He estimates the message encoded by Alice by using the quantum state in the quantum memory, the classical data in the classical memory and the basis disclosed by Alice. The whole process can be written as follows. The interaction between the qubits sent by Alice and Bob's apparatus is described by a completely positive map (CP-map),

$$\Lambda : \Sigma(\mathcal{H}_A) \to \Sigma(\mathcal{H}_m \otimes \mathcal{K}),$$

where $\Sigma(\mathcal{H})$ denotes a set of all density operators on $\mathcal{H}$. For instance, if Alice uses the basis Z for encoding message z, the state after the interaction becomes $\Lambda(|z\rangle\langle z|)$. Suppose that Bob obtained ξ as an outcome. The quantum state kept in the quantum memory depends on Z, z, and ξ, and is denoted by $\rho^Z_{z,\xi} \in \Sigma(\mathcal{H}_m)$, which can be calculated as an a-posteriori state [27]. We treat the quantum Kolmogorov complexity $K(z|\rho^Z_{z,\xi}, \xi, Z)$ as a measure to characterize Bob's estimation [28]. That is, if Bob can estimate z exactly only from what he actually has, $K(z|\rho^Z_{z,\xi}, \xi, Z) = O(1)$ holds. Otherwise, the quantum Kolmogorov complexity becomes nontrivial. Similarly, when Alice uses the basis X for encoding message x, and Bob obtains ξ as an outcome of the measurement on the auxiliary system, we denote the quantum state in the quantum memory by $\rho^X_{x,\xi} \in \Sigma(\mathcal{H}_m)$. $K(x|\rho^X_{x,\xi}, \xi, X)$ characterizes Bob's ability to estimate the message x [28].

When $M \geq N$ holds, Bob can recover the message perfectly by simply keeping the quantum states sent by Alice. We study how well Bob can recover the message when $M < N$ is satisfied.

In the following theorem, we study asymptotic behavior with respect to increasing N. For each N, the size of Bob's quantum memory M, which may depend on N, is bounded as $M \leq qN$ for some q $(0 \leq q \leq 1)$. For each N, $P(x|\xi_N, X)$ denotes a posterior probability of a message $x \in \{0,1\}^N$ when Alice used the basis X and Bob obtained outcome ξ_N. Similarly, $P(z|\xi_N, Z)$ denotes a posterior probability of a message $z \in \{0,1\}^N$ when Alice used the basis Z and Bob obtained ξ_N.

Theorem 3 *Let us consider a family of protocols indexed by the number of qubits N. Assume that for each N the size of Bob's quantum memory M, which may depend on N, is bounded as $M \leq qN$ for some q $(0 \leq q \leq 1)$. For any p_X and p_Z satisfying $q + p_X + p_Z < 1$, there exists $C_0 > 0$ and $\epsilon > 0$ such that for any ξ_N,*

$$P(\{x|K(x|\rho^X_{x,\xi_N}, \xi_N, X) \leq p_X N\}|\xi_N, X) + P(\{z|K(z|\rho^Z_{z,\xi_N}, \xi_N, Z) \leq p_Z N\}|\xi_N, Z) \leq 1 + C_0 2^{-\epsilon N}$$

holds for a sufficiently large N, where $P(\{x|K(x|\rho^X_{x,\xi_N}, \xi_N, X) \leq p_X N\}|\xi_N, X) := \sum_x^{K(x|\rho^X_{x,\xi_N}, \xi_N, X) \leq p_X N} P(x|\xi_N, X)$ and $P(\{z|K(z|\rho^Z_{z,\xi_N}, \xi_N, Z) \leq p_Z N\}|\xi_N, Z) := \sum_z^{K(z|\rho^Z_{z,\xi_N}, \xi_N, Z) \leq p_Z N} P(z|\xi_N, Z)$.

The above theorem shows that there is a non-trivial trade-off relation between $P(\{x|K(x|\rho^X_{x,\xi_N}, \xi_N, X) \leq p_X N\}|\xi_N, X)$ and $P(\{z|K(z|\rho^Z_{z,\xi_N}, \xi_N, Z) \leq p_Z N\}|\xi_N, Z)$ when $q + p_X + p_Z < 1$ holds. In particular, for sufficiently large N, if one of them is close to 1, the other becomes exponentially small. In other words, as there is a pair p_X and p_Z satisfying $q + p_X + p_Z < 1$ for any $q < 1$, there is a nontrivial effect of the bounded quantum memory for any $q < 1$.

The above theorem is derived from the following lemma.

Lemma 1 *Let us consider a protocol for a fixed N and M. For any integers $l_X, l_Z \geq 0$, it holds:*

$$P(\{x|K(x|\rho^X_{x,\xi}, \xi, X) \leq l_X\}|\xi, X) + P(\{z|K(z|\rho^Z_{z,\xi}, \xi, Z) \leq l_Z\}|\xi, Z) \leq 1 + 2^{\frac{l_X + l_Z + M - N}{2} + c},$$

where $P(\{x|K(x|\rho^X_{x,\xi}, \xi, X) \leq l_X\}|\xi, X) := \sum_x^{K(x|\rho^X_{x,\xi}, \xi, X) \leq l_X} P(x|\xi, X)$, $P(\{z|K(z|\rho^Z_{z,\xi}, \xi, Z) \leq l_Z\}|\xi, Z) := \sum_z^{K(z|\rho^Z_{z,\xi}, \xi, Z) \leq l_Z} P(z|\xi, Z)$ and c is a constant depending on the choice of a quantum Turing machine. (Note that this inequality is non-trivial only for $\frac{l_X + l_Z + M - N}{2} + c < 0$.)

Proof:

We fix a universal quantum Turing machine U and discuss the quantum Kolmogorov complexity with respect to it. We fix ξ throughout the proof. Let us consider $K_U(z|\rho^Z_{z,\xi}, \xi, Z)$ first. Thanks to theorem 2, it suffices to consider only programs that exactly output the message z because the message is a classical object. That is, we regard

$$K_{c,U}(z|\rho_z, Z) := \min_{q: U(q, \rho^Z_{z,\xi}, \xi, Z) = |z\rangle} l(q),$$

which satisfies $K_{c,U}(z|\rho^Z_{z,\xi}, \xi, Z) \geq K_U(z|\rho^Z_{z,\xi}, \xi, Z) \geq K_{c,U}(z|\rho^Z_{z,\xi}, \xi, Z) - c'$ for some constant c'.

Let us denote by $T^\xi_z \subset \{0,1\}^*$ a set of all programs that output z with auxiliary inputs $\rho^Z_{z,\xi}$, ξ and Z. That is, $T^\xi_z = \{t \in \{0,1\}^* | U(t, \rho^Z_{z,\xi}, \xi, Z) = z\}$ holds. An equation $K_{c,U}(z|\rho^Z_{z,\xi}, \xi, Z) = \min_{t \in T^\xi_z} l(t)$ follows. Although different programs may have different halting times, from the lemma proved by Müller (Lemma 2.3.4. in [20]), we note that there exists a completely positive map (CP-map) $\Gamma_{U,\xi,Z} : \Sigma(\mathcal{H}_m \otimes \mathcal{H}_I) \to \Sigma(\mathcal{H}_O)$ satisfying for any $t \in T^\xi_z$

$$\Gamma_{U,\xi,Z}(\rho^Z_{z,\xi} \otimes |t\rangle\langle t|) = |z\rangle\langle z|,$$

where $\mathcal{H}_I$ is a Hilbert space for programs, and $\mathcal{H}_O = \otimes^N \mathbf{C}_2$ is a Hilbert space for outputs. From this theorem, we obtain an important observation. If $T_z^\xi \cap T_{z'}^\xi \neq \emptyset$ holds for some $z \neq z'$, $\rho_{z,\xi}^Z$ and $\rho_{z',\xi}^Z$ are perfectly distinguishable. In fact, because a CP-map does not increase the distinguishability of states, the relationships for $t \in T_z^\xi \cap T_{z'}^\xi$

$$\Gamma_{U,\xi,Z}(\rho_{z,\xi}^Z \otimes |t\rangle\langle t|) = |z\rangle\langle z|$$
$$\Gamma_{U,\xi,Z}(\rho_{z',\xi}^Z \otimes |t\rangle\langle t|) = |z'\rangle\langle z'|$$

and their distinguishability on the right-hand sides imply the distinguishability of $\rho_{z,\xi}^Z$ and $\rho_{z',\xi}^Z$. For each $t \in \{0,1\}^*$, we define $\mathcal{C}_t^\xi \subset \{0,1\}^N$ as $\mathcal{C}_t^\xi = \{z | t \in T_z\}$. That is, $z \in \mathcal{C}_t^\xi$ is a message that can be reconstructed by giving a program t to the Turing machine U with auxiliary inputs $\rho_{z,\xi}^Z$, ξ and Z. Owing to the distinguishability between $\rho_{z,\xi}^Z$ and $\rho_{z',\xi}^Z$, for $z, z' \in \mathcal{C}_t^\xi$, there exists a family of projection operators $\{E_z^{t,\xi}\}_{z \in \mathcal{C}_t^\xi}$ on $\mathcal{H}_m$ satisfying for any $z, z' \in \mathcal{C}_t^\xi$,

$$E_z^{t,\xi} E_{z'}^{t,\xi} = \delta_{zz'} E_z^{t,\xi}$$
$$\sum_{z \in \mathcal{C}_t^\xi} E_z^{t,\xi} \leq \mathbf{1}$$
$$\mathrm{tr}(\rho_z E_{z'}^{t,\xi}) = \delta_{zz'}.$$

Because the memory is bounded as $\dim \mathcal{H}_m \leq 2^M$,

$$\left|\mathcal{C}_t^\xi\right| \leq 2^M$$

holds. Because we are interested in minimum length programs, we define $\mathcal{D}_t^\xi := \{z | t = \mathrm{argmin}_{s \in T_z^\xi} l(s)\}$, which is a set of all messages that have t as the minimum length program for reconstruction. $\mathcal{D}_t^\xi \subset \mathcal{C}_t^\xi$ holds. It is still possible that $\mathcal{D}_t^\xi \cap \mathcal{D}_{t'}^\xi \neq \emptyset$. That is, there may be a message z whose shortest programs are not unique. In such a case, we choose one of these programs to avoid counting doubly. For instance, this can be done by introducing a total order $<$ in all the programs $\{0,1\}^*$, and by defining $\mathcal{E}_t^\xi = \{z | z \in \mathcal{D}_t^\xi, z \notin \mathcal{D}_{t'}^\xi \text{ for all } t' < t \text{ with } l(t) = l(t')\}$. As this $\mathcal{E}_t^\xi$ is a subset of $\mathcal{C}_t^\xi$, for any $z, z' \in \mathcal{E}_t^\xi$

$$E_z^{t,\xi} E_{z'}^{t,\xi} = \delta_{zz'} E_z^{t,\xi} \tag{1}$$
$$\sum_{z \in \mathcal{E}_t^\xi} E_z^{t,\xi} \leq \mathbf{1} \tag{2}$$
$$\mathrm{tr}(\rho_z E_{z'}^{t,\xi}) = \delta_{zz'}$$

hold. The cardinality of $\mathcal{E}_t^\xi$ satisfies

$$\left|\mathcal{E}_t^\xi\right| \leq 2^M. \tag{3}$$

Similarly, we treat $K_U(x|\rho_{x,\xi}^X, \xi, X)$. We can introduce $S_x^\xi \subset \{0,1\}^*$ as a set of all programs that output x with auxiliary inputs $\rho_{x,\xi}^X$, ξ, and X. $K_{c,U}(x|\rho_{x,\xi}^X, \xi, X) = \min_{s \in S_x^\xi} l(s)$ holds. We can define $\mathcal{J}_s^\xi := \{x | s \in S_x^\xi\}$ for each s and introduce a family of projection operators $\{F_x^{s,\xi}\}_{x \in \mathcal{F}_s^\xi}$ on $\mathcal{H}_m$ that satisfies

$$\mathrm{tr}(F_x^{s,\xi} \rho_{x',\xi}^X) = \delta_{xx'}$$

for each $x, x' \in \mathcal{J}_s^\xi$ and so on. $\mathcal{G}_s^\xi := \{x | s = \mathrm{argmin}_{t \in S_x^\xi} l(t)\}$ and $\mathcal{F}_s^\xi = \{z | z \in \mathcal{G}_s^\xi, z \notin \mathcal{G}_{s'}^\xi \text{ for all } s' < s \text{ with } l(s) = l(s')\}$, are also defined. An inequality for the cardinality,

$$\left|\mathcal{F}_s^\xi\right| \leq \left|\mathcal{J}_s^\xi\right| \leq 2^M \tag{4}$$

also holds. We consider a family of projection operators $\{F_x^{s,\xi}\}_{x \in \mathcal{F}_s^\xi}$.

Let us analyze the protocol. Instead of the original protocol, we treat an entanglement-based protocol (E91-like protocol [29]), which is equivalent to the original one. It runs as follows. Alice prepares N pairs of qubits. She prepares each pair in the EPR state, $|\phi\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. Therefore, the whole state can be written as

$|\phi^N\rangle := |\phi\rangle \otimes |\phi\rangle \otimes \cdots \otimes |\phi\rangle$ (N times) in a Hilbert space $\mathcal{H}_{A'} \otimes \mathcal{H}_A$, where $\mathcal{H}_{A'} \simeq \mathcal{H}_A \simeq \otimes^N \mathbf{C}^2$. Alice sends the qubits described by $\mathcal{H}_B$ to Bob. Bob makes the system $\mathcal{H}_A$ interact with his apparatus as

$$\Lambda : \Sigma(\mathcal{H}_A) \to \Sigma(\mathcal{H}_m \otimes \mathcal{K}).$$

Bob measures his auxiliary system $\mathcal{K}$ with POVM $C = \{C_\xi\}$. When Bob has obtained ξ, we denote by Θ_ξ the a-posteriori state [27] over $\mathcal{H}_{A'} \otimes \mathcal{H}_m$. Alice measures her system $\mathcal{H}_{A'}$ with one of the bases X or Z to obtain a message. It can be shown that when Bob's obtained outcome was ξ and Alice chose X and obtained x, the state on the quantum memory $\mathcal{H}_m$ is $\rho^X_{x,\xi}$. Similarly, when Bob's obtained outcome was ξ and Alice chose Z and obtained z, the state on the quantum memory $\mathcal{H}_m$ is $\rho^Z_{z,\xi}$.

Hereafter we treat the state Θ_ξ over $\mathcal{H}_{A'} \otimes \mathcal{H}_m$. Let us define a projection operator for each $t \in \{0,1\}^*$, $P^\xi_t := \sum_{z \in \mathcal{E}^\xi_t} Z_z \otimes E^{t,\xi}_z$, and for each $s \in \{0,1\}^*$, $Q^\xi_s := \sum_{x \in \mathcal{F}^\xi_s} X_x \otimes F^{s,\xi}_x$. For any integers $l'_X, l'_Z \geq 0$, we introduce projection operators, $\hat{P}^\xi_{l'_Z} := \sum_t^{l(t) \leq l'_Z} P^\xi_t$ and $\hat{Q}^\xi_{l'_X} := \sum_s^{l(s) \leq l'_X} Q^\xi_s$. Their expectation values with respect to Θ_ξ can be written as:

$$\mathrm{tr}(\Theta_\xi \hat{P}^\xi_{l'_Z}) = P\left(\{z | K_{c,U}(z|\rho^Z_{z,\xi}, \xi, Z) \leq l'_Z\} | \xi, Z\right) \tag{5}$$

$$\mathrm{tr}(\Theta_\xi \hat{Q}^\xi_{l'_X}) = P\left(\{x | K_{c,U}(x|\rho^X_{x,\xi}, \xi, X) \leq l'_X\} | \xi, X\right). \tag{6}$$

Our purpose is to find a trade-off inequality between (5) and (6). It is obtained by the use of the uncertainty relation, which is one of the most important relation characterizing quantum mechanics. Among the various forms of uncertainty relations, we employ the Landau-Pollak uncertainty relation [30, 31]. According to the generalized form given in [31], for an arbitrary number of projections $\{A_i\}$, it holds that for any quantum state ρ,

$$\sum_i \mathrm{tr}(\rho A_i) \leq 1 + \left(\sum_{i \neq j} \|A_i A_j\|^2 \right)^{1/2}.$$

We apply this inequality for the state Θ_ξ and a family of positive operators $\{P_t, Q_s\}$ ($l(t) \leq l'_Z, l(s) \leq l'_X$). Because $P_t P_{t'} = Q_s Q_{s'} = 0$ holds for $t \neq t'$ and $s \neq s'$ thanks to $\mathcal{E}^\xi_t \cap \mathcal{E}^\xi_{t'} = \mathcal{F}^\xi_s \cap \mathcal{F}^\xi_{s'} = \emptyset$, we obtain:

$$\mathrm{tr}(\Theta_\xi \hat{P}^\xi_{l'_Z}) + \mathrm{tr}(\Theta_\xi \hat{Q}^\xi_{l'_X}) \leq 1 + \left(2 \sum_t^{l(t) \leq l'_Z} \sum_s^{l(s) \leq l'_X} \|Q^\xi_s P^\xi_t\|^2 \right)^{1/2}.$$

The term $\|Q^\xi_s P^\xi_t\|$ on the right-hand side is computed as follows. As the operator norm $\|Q^\xi_s P^\xi_t\|$ is written as $\|Q^\xi_s P^\xi_t\| = \sup_{|\Psi\rangle : \||\Psi\rangle\| = 1} \|Q^\xi_s P^\xi_t |\Psi\rangle\|$, we need to bound $\|Q^\xi_s P^\xi_t |\Psi\rangle\|$ for any normalized vector $|\Psi\rangle$. We consider:

$$\|Q^\xi_s P^\xi_t |\Psi\rangle\| = \langle \Psi | P^\xi_t Q^\xi_s P^\xi_t |\Psi\rangle^{1/2}. \tag{7}$$

As $Q^\xi_s = \sum_{x \in \mathcal{F}^\xi_s} X_x \otimes F^{s,\xi}_x \leq \sum_{x \in \mathcal{F}^\xi_s} X_x \otimes \mathbf{1}_M$ holds, (7) can be bounded as

$$\begin{aligned} \langle \Psi | Q^\xi_s P^\xi_t Q^\xi_s |\Psi\rangle^{1/2} &\leq \left(\sum_{z \in \mathcal{E}^\xi_t} \sum_{x \in \mathcal{F}^\xi_s} \sum_{z' \in \mathcal{E}^\xi_t} \langle \Psi | (Z_z \otimes E^{t,\xi}_z)(X_x \otimes \mathbf{1}_M)(Z_{z'} \otimes E^{t,\xi}_{z'}) |\Psi\rangle \right)^{1/2} \\ &= \left(\sum_{z \in \mathcal{E}^\xi_t} \sum_{x \in \mathcal{F}^\xi_s} \langle \Psi | Z_z X_x Z_z \otimes E^{t,\xi}_z |\Psi\rangle \right)^{1/2}, \end{aligned}$$

where we have used (1). The right-hand side can be further deformed by introducing the a-posteriori state [27] $\mu^{t,\xi}_z$

as:

$$\left(\sum_{z\in\mathcal{E}_t^\xi}\sum_{x\in\mathcal{F}_s^\xi}\langle\Psi|Z_zX_xZ_z\otimes E_z^{t,\xi}|\Psi\rangle\right)^{1/2} = \left(\sum_{z\in\mathcal{E}_t^\xi}\sum_{x\in\mathcal{F}_s^\xi}\mathrm{tr}(\mu_z^{t,\xi}Z_zX_xZ_z)\langle\Psi|\mathbf{1}_B\otimes E_z^{t,\xi}|\Psi\rangle\right)^{1/2}$$
$$\leq \left(\sum_{z\in\mathcal{E}_t^\xi}\sum_{x\in\mathcal{F}_s^\xi}\frac{1}{2^N}\langle\Psi|\mathbf{1}_B\otimes E_z^{t,\xi}|\Psi\rangle\right)^{1/2}$$
$$\leq \left(\frac{1}{2^N}|\mathcal{F}_s^\xi|\right)^{1/2}\leq 2^{\frac{M-N}{2}},$$

where we have used a relation $|\mathrm{tr}(\mu_z^{t,\xi}Z_zX_xZ_z)|\leq\|Z_zX_xZ_z\|=\frac{1}{2^N}$, (2) and (4). Thus we obtain $\|Q_s^\xi P_t^\xi\|\leq 2^{\frac{M-N}{2}}$. Because $|\{t|l(t)\leq l'_Z\}|\leq 2^{l'_Z+1}$ and $|\{s|l(s)\leq l'_X\}|\leq 2^{l'_X+1}$ hold, we obtain

$$\mathrm{tr}(\Theta_\xi\hat{P}_{l'_Z}^\xi)+\mathrm{tr}(\Theta_\xi\hat{Q}_{l'_X}^\xi)\leq 1+2^{\frac{l'_X+l'_Z+M-N+3}{2}}.$$

Taking into account the relation between $K_{c,U}$ and K_U we finally obtain:

$$P(\{x|K(x|\rho_{x,\xi}^X,\xi,X)\leq l_X\}|\xi,X)+P(\{z|K(z|\rho_{z,\xi}^Z,\xi,Z)\leq l_Z\}|\xi,Z)\leq 1+2^{\frac{l_X+l_Z+M-N}{2}+c},$$

where c is a constant that depends on the choice of the quantum Turing machine. Q.E.D.

Proof of theorem 3: Apply lemma 1 with $l_X=p_XN$, $l_Z=p_ZN$ and $M=qN$. As c does not depend on N, we define $C_0:=2^c$. If we define $\epsilon:=\frac{1-(q+p_X+p_Z)}{2}$, we obtain the theorem. Q.E.D.

In addition, the following corollary immediately follows:

Corollary 1 *Let us consider a protocol with fixed N. For any memory size $M\geq 0$ and any ξ, it holds*

$$\max_{x:P(x|\xi,X)\neq 0}K(x|\rho_{x,\xi}^X,\xi,X)+\max_{z:P(z|\xi,Z)\neq 0}K(z|\rho_{z,\xi}^Z,\xi,Z)\geq N-M+c.$$

Proof: From $P(\{x|K(x|\rho_{x,\xi}^X,\xi,X)\leq\max_x K(x|\rho_{x,\xi}^X,\xi,X)\}|\xi,X)=1$, $P(\{z|K(z|\rho_{z,\xi}^X,\xi,Z)\leq\max_z K(z|\rho_{z,\xi}^Z,\xi,Z)\}|\xi,Z)=1$, and the lemma 1, the claim immediately follows. (For $M=0$, it also holds.) Q.E.D.

This corollary is regarded as a kind of generalizations of Heisenberg's uncertainty principle [32]. In fact, the case $M=0$ corresponds to the standard measurement scenario without a quantum memory. It implies that there is no observable that works as the joint measurement of X and Z.

IV. DISCUSSION

In this study, the power of the bounded quantum memory in simple information processing was examined. A toy two-party protocol was employed in which Bob, by using a bounded quantum memory and an unbounded classical memory, estimated messages encoded by Alice in one of the bases X or Z. His ability to guess the message was characterized by the quantum Kolmogorov complexity. Our theorem provided a nontrivial effect of the memory boundedness. In addition, as a corollary, we obtained a generalization of the uncertainty principle with the quantum memory. As a future problem, it would be natural to apply the present study to the oblivious transfer. It should be noted that in [7], non-trivial result was obtained only for the quantum memory smaller than $N/2$ in the context of oblivious transfer, whereas our result indicates that there may be a non-trivial effect also for the quantum memory for which the size is qN for some $q<1$. To investigate the complete protocol, we need to treat privacy amplification by using the Kolmogorov complexity. In addition, by combining the present result with the information-disturbance theorem [11] in quantum key distribution, our theorem may play a role in estimating the threat of an eavesdropper who has a bounded quantum memory. We hope to investigate these problems in the future.

[1] M. O. Rabin, Technical Report TR-81, Aiken Computation Laboratory, Harvard University 1981.

[2] H. K. Lo and H. F. Chau, Phys. Rev. Lett. **78(17)**, 3410 (1997).
[3] D. Mayers, Phys. Rev. Lett. **78(17)**, 3414 (1997).
[4] C. Crepeau and J. Kilian, in 29th Annual IEEE Symposium on Foundation of Computer Science (FOCS), 42 (1988).
[5] I. B. Damgaard, S. Fehr, K. Morozov, and L. Salvail, in Theory of Cryptography Conference (TCC), LNCS **2951**, 355 (2004).
[6] C. Cachin, C. Crepeau, and J. Marcil, in 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 493 (1998).
[7] I. B. Damgaard, S. Fehr, L. Salvail, and C. Schaffner, in *Proceedings of the 46th IEEE Symposium on Foundations of Computer Science* 2005, p.449.
[8] C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India*, 1984, p.175.
[9] P. M. B. Vitányi, IEEE Trans. Inform. Theory **47 (6)**, 2464 (2001).
[10] T. Miyadera and H. Imai, Phys. Rev. A **79**, 012324 (2009).
[11] T. Miyadera, *arXiv: 1101.2946*, (2011).
[12] A. N. Kolmogorov, Probl. Inform. Transm. **1 (1)**, 1 (1965).
[13] G. Chaitin, J. Assoc. Comput. Mach. **13**, 547 (1966).
[14] M. Li and P. M. B. Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag: New York, 1997.
[15] G. Chaitin, *Algorithmic information theory*, Cambridge university press: Cambridge, 1987.
[16] K. Svozil, J. of Universal Comput. Sci. **2**, 311 (1996).
[17] A. Berthiaume, W. van Dam and S. Laplante, J. Comput. System. Sci. **63**, 201 (2001),
[18] P. Gacs, J. Phys. A: Math. Gen. **34**, 1 (2001),
[19] M. Müller, IEEE Trans. Inform. Theory **54 (2)**, 763 (2008).
[20] M. Müller, Ph.D. thesis 2007.
[21] A. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997).
[22] J. M. Myers, Phys. Rev. Lett. **78**, 1823 (1997).
[23] N. Linden and S. Popescu, *quant-ph/9806054*, (1998).
[24] M. Ozawa, Phys. Rev. Lett. **80**, 631 (1998).
[25] T. Miyadera and M. Ohya, Open Sys. Info. Dyn. **12**, 261 (2005).
[26] The word "probabilistically" here is used to mean "randomly in a probabilistic sense". That is, we use an unbiased probability $1/|\Omega|$ to choose a sample from a sample space Ω (say $\Omega = \{0,1\}^{2N}$). (To avoid a possible confusion of it with randomness in algorithmic sense, we just write "probabilistically".)
[27] In general, a-posteriori state after a measurement is determined as follows. Suppose that there exist two system A and B that are described by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Let us consider a state ρ over the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$. Suppose that on A one made a measurement described by a POVM $F = \{F_x\}$ and obtained an outcome x. A-posteriori state on the system B conditioned with this x becomes

$$\rho_x = \frac{\mathrm{tr}_A(\rho(F_x \otimes \mathbf{1}))}{\mathrm{tr}\rho F_x \otimes \mathbf{1})}.$$

That is, it is a unique state that satisfies $\mathrm{tr}(\rho_x G)\mathrm{tr}(\rho(F_x \otimes \mathbf{1})) = \mathrm{tr}(\rho(F_x \otimes G))$ for any operator G on $\mathcal{H}_B$.
[28] To treat $\rho^Z_{z,\xi}$ and $\rho^X_{x,\xi}$ as an auxiliary input for a quantum Turing machine, they have to be somehow represented as states on a system consisting of qubits. Our discussion does not depend on how we identify them.
[29] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[30] H. Maassen and J. B. M. Uffink, Phys.Rev.Lett. **60**, 1103 (1988).
[31] T. Miyadera and H. Imai, Phys. Rev. A **76**, 062108 (2007).
[32] T. Miyadera and H. Imai, Phys. Rev. A **78**, 052119 (2008).